



## Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

### EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019

Date filed: Friday, March 1st, 2019

Name of company covered by this certification: CoMedia Communications, Inc.

Form 499 Filer ID: 826193

Name of signatory: David D. Young

Title of signatory: President and CEO


I, David D. Young, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

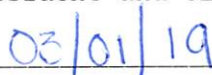
The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

  
David D. Young  
President and CEO

Dated





**COMEDIA COMMUNICATIONS, INC.  
CUSTOMER PROPRIETARY NETWORK INFORMATION  
STATEMENT**

CoMedia Communications, Inc. respects our subscribers' right to maintain the confidentiality of their individual Customer Proprietary Network Information ("CPNI"). CoMedia Communications, Inc. has a duty to protect the confidentiality of such CPNI and maintains the following policy to safeguard our subscribers' CPNI:

**I. CPNI Utilization**

- The Company discloses, and permits access to CPNI to protect our rights and property, the Company's subscribers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, the Company's services.
- The Company uses, discloses, and permits access to CPNI to initiate, render, bill and collect for its telecommunications services.
- The Company uses, discloses and permits access to CPNI to provide or market service offerings related to the same category of service to which a subscriber presently subscribes.
- The Company uses, discloses, and permits access to CPNI a) to provide inside wiring installation, maintenance and repair services; and b) in the event that we provide local services to a subscriber, to market services formerly known as adjunct to basic services, including, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features.
- The Company discloses CPNI to any person designated by a subscriber upon receipt of an affirmative written request by the subscriber.
- The Company does not disclose or release subscriber call detail information to anyone on a subscriber initiated call unless the subscriber provides a pre-established password, the subscriber requested information is sent to the address on record, or the Company calls the subscriber telephone number of record and discloses the information.
- The Company does not use CPNI to market Internet access services or to identify or track subscribers who call competitive service providers.
- The Company discloses CPNI to law enforcement upon receiving an authorized request for such information from a law enforcement agency.

**II. CPNI Approvals**

- When subscriber approval to use, disclose or permit access to subscriber CPNI is required, the Company obtains approval through written opt-in methods. The Company honors a subscriber's approval or disapproval until the subscriber revokes or limits such approval or disapproval. Records of subscriber approvals are maintained for one year.

**III. CPNI Safeguards**



- The Company's Controller maintains a record of any marketing campaigns utilizing subscribers' CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign and what products and services were offered as part of the campaign. Any such marketing campaigns must be approved by the President and CEO. These records are maintained for one year.
- The Company's Controller maintains a listing of subscribers and their CPNI disclosure approval status.
- The Company trains its personnel on the CPNI requirements on an on-going basis.
- The Company will notify the US Secret Service and the FBI within seven business days of a breach in CPNI. Unless law enforcement officials prohibit notification, subscribers will be notified within seven more business days unless there is immediate danger or harm to the subscriber, which triggers immediate notification. The notification to the US Secret Service and the FBI shall be in the form of a letter and shall include the Company's name, a description of the breach in CPNI, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission has been notified and whether it has taken any action, a copy of the notice provided to subscribers, and contact information. Records of breaches will be kept for two years.
- The subscriber's password may not be established on a subscriber-initiated call. Passwords may not consist of available biographical information such as social security number, telephone number or subscriber name.
- The Company has updated its business subscriber contracts/policies to include certain CPNI security procedures.
- When there is a request to change the password, telephone number of record or online account information or address of record, a notice is sent to the old address advising that a change request has been received. This notice does not contain the new address or password. If the subscriber believes that this change is unauthorized, the subscriber is to contact the Company immediately.
- Should a subscriber request records or information from the Company that contains CPNI, such information will only be provided if (1) the subscriber provides a pre-established password, or (2) the information is mailed to the address of record or (3) the Company calls the subscriber back at the phone number of record and discloses the requested information or (4) the request is made in person at a Company office and the subscriber presents a drivers license or other government issued photo identification that proves that the request is the subscriber of record.